

REMARKS

This Application has been carefully reviewed in light of the Office Action mailed November 27, 2000. In order to advance prosecution of this Application, Applicant has responded to each notation by the Examiner. Applicant respectfully requests reconsideration, further examination, and favorable action in this case.

I. RESPONSE TO THE EXAMINER'S "SUMMARY OF THE INVENTION"

The Examiner "summarized" Applicant's invention in the Office Action. (*Summary of the Invention, Page 7, Paragraph D*). Applicant objects to the Examiner's characterization of the invention to the extent that it is inconsistent with the claims and/or specification. Also, Applicant acknowledges that the Examiner may refuse to give patentable weight to a recitation of intended use in the preamble of a claim (*M.P.E.P. § 2111.02, entitled "Weight of Preamble"*). However, Applicant respectfully notes that the Examiner may not ignore actual claims elements outside the preamble of the claim. (*See, e.g., M.P.E.P. § 2131, "A claim is anticipated only if each and every element ... is found"*).

II. OBJECTIONS

A. THE TITLE IS DESCRIPTIVE OF THE CLAIMED INVENTION

The Examiner objected to the title of the invention as "not descriptive" because the current title is "directed to a family of devices." Applicant respectfully notes that the title of the Application only needs to be "clearly indicative of the invention to which the claims are directed." (*M.P.E.P. § 606.01*). Applicant also notes that the title of the Application is similar to the preambles of the independent claims, so the title is clearly indicative of the invention to which the claims are directed. Applicant respectfully requests withdrawal of the objection.

B. THE DRAWINGS SHOW EVERY FEATURE OF THE CLAIMED INVENTION

The Examiner objected to the drawings as failing to show every feature of the claimed invention. Applicant submits two new figures, Figure 7 and Figure 8. Applicant also amends the Specification to include a description of new Figures 7 and 8. Applicant submits that no new

matter is included with these figures. Applicant respectfully requests entry and acceptance of the figures and withdrawal of the objection.

III. 35 U.S.C. § 112 REJECTIONS

A. THE CLAIMS RECITE STATUTORY SUBJECT MATTER

The Examiner rejected Claims 7-15 under 35 U.S.C. § 101 as reciting non-statutory subject matter. Applicant has amended Claims 7 and 13. Applicant submits that Claims 7 and 13 recite patentable subject matter. Applicant respectfully requests withdrawal of the rejection of Claims 7 and 13, and Claims 9-12 and 14-15 depending therefrom.

B. THE CLAIMS ARE ENABLED BY APPLICANT'S DISCLOSURE

The Examiner rejected Claims 1-6 under 35 U.S.C. § 112, first paragraph. The Examiner asserted that Applicant has not enabled "automatically providing ... access privileges" in Applicant's specification. Applicant respectfully traverses this rejection. Applicant's specification provides enough information to teach a person of ordinary skill in the art how to make and use Applicant's claimed invention.

The burden falls on the Examiner to establish a "reasonable basis to question the enablement provided for the claimed invention." (*M.P.E.P.* § 2164.04). A specification that "contains a teaching of the manner and process of making and using an invention in terms which correspond in scope to those used in describing and defining the subject matter sought to be patented must be taken as being in compliance with the enablement requirement of 35 U.S.C. 112, first paragraph, unless there is reason to doubt the objective truth of statements contained therein which must be relied on for enabling support." (*M.P.E.P.* § 2164.04). The Patent Office must "explain *why* it doubts the truth or accuracy of any statement in a supporting disclosure and to back up assertions of its own with acceptable evidence or reasoning which is inconsistent with the contested statement." (*M.P.E.P.* § 2164.04).

Claims 1-6 recite a method of providing access privileges to records of members of a community. Applicant's disclosure enables one skilled in the art to perform the claimed method.

In the Application, Figure 4 illustrates one embodiment of a method for “generating [a] list of authorized functions” in Applicant’s described system. (*Specification, Page 23, Lines 21-22*). The authorized functions are “functions that may be performed by the user in the system.” (*Specification, Page 11, Lines 21-23*). Figure 5 illustrates one embodiment of a method for “generating a list of authorized objects.” (*Specification, Page 23, Lines 21-22*). The authorized objects may identify “members of the community related to the user such that the user is authorized to access records of those members.” (*Specification, Page 12, Lines 4-7*). The process of identifying the authorized objects may include the use of the authorized functions identified using the method illustrated in Figure 4. (*Specification, Page 25, Lines 6-18*). Figures 6 and 7 illustrate two embodiments of methods for “authorizing access to records of members of the community.” (*Specification, Page 27, Lines 21-22; Page 31, Lines 25-28*). The process of authorizing access to the records may include the use of the authorized objects identified using the method of Figure 5. (*Specification, Page 27, Lines 23-28*). Overall, Figures 4-7 illustrate one embodiment of how a system may provide access privileges to records of members of a community.

The above-cited portions of Applicant’s specification, along with the rest of the Application, enable one of skill in the art to make and use Applicant’s claimed invention. In particular, Applicant’s specification describes how to construct a system that may “automatically provide ... access privileges” to a user. The Examiner has not explained why Applicant’s specification fails to enable any element of the claims, nor has the Examiner established any reason to “doubt the objective truth of statements contained” in Applicant’s specification. The Examiner has not presented “evidence or reasoning” which is inconsistent with the statements in the Application. Instead, the Examiner merely makes an unsupported assertion that the claims are not enabled. This falls far short of meeting the Examiner’s burden of establishing a “reasonable basis to question the enablement provided for the claimed invention.” As a result, Applicant respectfully requests withdrawal of the rejection of Claim 1, and Claims 2-6 depending therefrom.

The Examiner also rejected Claims 7-15 under 35 U.S.C. § 112, first paragraph. The Examiner asserted that because Claims 7-15 lack utility under 35 U.S.C. § 101, a person of skill in the art would not know how to use the claimed invention. As described above, Applicant submits that Amended Claims 7 and 13 recite patentable subject matter and comply with 35 U.S.C. § 101. As a result, Applicant respectfully submits that a person skilled in the art would know how to use Applicant's claimed invention. Applicant respectfully requests withdrawal of the rejection of Claims 7 and 13, and Claims 9-12 and 14-15 depending therefrom.

C. THE CLAIMS PARTICULARLY POINT OUT AND DISTINCTLY CLAIM THE INVENTION

The Examiner rejected Claims 7-15 under 35 U.S.C. § 112, second paragraph, as indefinite. Applicant has amended Claims 7 and 13. Applicant submits that Claims 7 and 13 particularly point out and distinctly claim Applicant's invention. Applicant respectfully requests withdrawal of the rejection of Claims 7 and 13, and Claims 9-12 and 14-15 depending therefrom.

IV. 35 U.S.C. § 102 REJECTIONS

The Examiner rejected Claims 1-15 under 35 U.S.C. §§ 102(b) and 102(e), as being unpatentable over seven different references. Applicant respectfully traverses these rejections for the reasons discussed below.

A. PIECEMEAL EXAMINATION OF THE APPLICATION SHOULD BE AVOIDED

Applicant notes that the Examiner rejected all of the pending claims under seven (7) separate 35 U.S.C. § 102 rejections. In accordance with the Manual of Patent Examining Procedure (*M.P.E.P.*), such piecemeal examination should be avoided as much as possible. "The Examiner ordinarily should reject each claim on all valid grounds available, avoiding, however, undue multiplication of references." (*M.P.E.P.* § 707.07(g), entitled "*Piecemeal Examination*"). Accordingly, should the Examiner continue the rejection of any of the pending claims, Applicant respectfully requests that the Examiner limit such rejections to the best available art in order to not unduly burden Applicant in responding to any such rejection. However, as discussed below,

Applicant submits that the claims are not anticipated or made obvious by any of the cited references.

B. THE CLAIMS ARE PATENTABLE OVER HOWELL AND ABRAHAM

The Examiner rejected Claims 1-15 under 35 U.S.C. § 102(b), as being unpatentable over U.S. Patent No. 5,276,901 issued to Howell et al. ("*Howell*") and U.S. Patent No. 5,446,903 issued to Abraham et al. ("*Abraham*"). Applicant respectfully traverses these rejections for the reasons discussed below.

Howell and *Abraham* each discloses a system that combines users of a database into groups of users. Access to an object in the system may then be granted to individual users and to groups of users.

Howell discloses a system for controlling access by groups of users to an object. (*Abstract*). In the system of *Howell*, an "access list" is associated with an object, and it identifies which users or groups are allowed to access that object. (*Col. 2, lines 33-42*). An "access folder" is associated with a user or a group, and it defines the privileges that the user or group has with respect to an object. (*Col. 5, lines 23-30; Col. 7, lines 32-50*). A user of the system may gain access to an object in two ways. First, if the user is explicitly listed in an object's access list, the user can access the object. (*Col. 2, lines 42-48*). Second, the user may belong to a group that is allowed to access an object. The system determines if a group is listed in the object's access list, and if so the system determines whether that group's access folder is listed in the user's access folder. (*Col. 7, lines 58-68*). Therefore, *Howell* teaches grouping users together and allowing groups to access an object.

Abraham teaches a system for maintaining security based on the current status of an industrial process. (*Abstract*). The industrial process typically includes a series of processing steps. (*Col. 1, lines 16-18*). *Abraham* protects data elements in the system by combining users into groups. (*Col. 3, lines 1-10*). *Abraham* then allows predetermined groups of users to access data elements in the system based on the processing step currently active in the industrial process.

(Col. 3, lines 1-10). If the industrial process is not at a particular processing step, a group of users may be prevented from accessing data elements in the system. (Col. 3, lines 11-15).

Both *Howell* and *Abraham* allow a system to combine users into groups, and the system then allows the groups to access objects. *Abraham* adds the additional feature of limiting a group's access based on the current processing step of an industrial process. *Howell* and *Abraham* both fail to teach or suggest granting one member of the community access privileges to the records of another member. In particular, *Howell* and *Abraham* lack any teaching or suggestion of giving one member access privileges to the records of another member based on a management or other type of relationship between those members. *Howell* and *Abraham* also lack any teaching or suggestion of "automatically" providing access privileges based on relationships between members of the community. Because of this, *Howell* and *Abraham* fail to teach or suggest Claims 1, 7, 13, and 16-19.

For example, *Howell* and *Abraham* teach grouping users together and then allowing the group to access an object. There is no teaching or suggestion in *Howell* or *Abraham* of assigning a single member of a community to multiple positions in the community and then automatically providing managers of the positions with disparate levels of access to the member's records. As a result, *Howell* and *Abraham* fail to teach or suggest storing "an assignment of a member ... to a first position" and "an additional assignment of the member to a second position" as recited in Claims 1, 16, and 17. *Howell* and *Abraham* also fail to teach or suggest automatically providing "a manager of the first position with access privileges to records of the member" and "a manager of the second position with disparate access privileges to records of the member" as recited in Claims 1, 16, and 17. As a result, *Howell* and *Abraham* fail to teach or suggest Claims 1, 16, and 17.

There is also no teaching or suggestion in *Howell* or *Abraham* of assigning one management position to another management position and then automatically providing a first member with at least a portion of a second member's access privileges based on the assignment. As a result, *Howell* and *Abraham* fail to teach or suggest storing "a first assignment of a first

member .. to a first manager position,” “a second assignment of a second member ... to a second manager position,” and “a third assignment of the first manager position to the second manager position” as recited in Claims 7, 18, and 19. *Howell* and *Abraham* also fail to teach or suggest providing “the first member with at least a portion of the access privileges of the second member” as recited in Claims 7, 18, and 19. In addition, because *Howell* and *Abraham* fail to teach or suggest giving one member access to the records of another member based on a management relationship between the members, *Howell* and *Abraham* fail to teach or suggest granting a first member at least a portion of the access privileges of a second member, where the access privileges comprise “access privileges to records of members of the community reporting to the” second member. As a result, *Howell* and *Abraham* fail to teach or suggest Claims 7, 18, and 19.

In addition, *Howell* and *Abraham* fail to teach or suggest giving one member access to the records of another member based on any type of relationship between the members. *Howell* and *Abraham* therefore fail to teach or suggest a processor operable to provide a first member and a second member with disparate access privileges to records of a third member based on “recorded assignments” of the “members of the community to positions in the community.” As a result, *Howell* and *Abraham* fail to teach or suggest Claim 13.

For at least these reasons, Applicant respectfully requests withdrawal of the rejections and full allowance of Claims 1, 7, 13, and 16-19, and Claims 2-6, 9-12, 14, and 15 depending therefrom.

C. THE CLAIMS ARE PATENTABLE OVER BALDWIN, DEMURJIAN, AND BARKLEY

The Examiner rejected Claims 1-15 under 35 U.S.C. § 102(b), as being unpatentable over Baldwin, “Naming and Grouping Privileges to Simplify Security Management in Large Databases” (“*Baldwin*”) and Demurjian, “Towards and Authorization Mechanism for User-Role Based Security in an Object-Oriented Design Model.” (“*Demurjian*”). The Examiner also rejected Claims 1-15 under 35 U.S.C. § 102(e), as being unpatentable over U.S. Patent No.

6,088,679 issued to Barkley ("*Barkley*"). Applicant respectfully traverses these rejections for the reasons discussed below.

Baldwin, *Demurjian*, and *Barkley* each discloses a system that combines database privileges into groups of privileges. Access to objects may then be granted to a user of the system by assigning the group of privileges to the user.

Baldwin teaches a system that uses named protection domains ("NPDs"), which are groups of privileges. (*Page 116, Abstract*). An "object privilege" defines an individual user's ability to perform a specified operation on a particular object, and object privileges can be grouped together to form an NPD. (*Page 118, Left column, Second paragraph; Page 119, Left column, Fifth paragraph*). As one example, *Baldwin* teaches using role based security, which groups privileges together and forms an NPD according to the job that a user performs. (*Page 120, Left column, Fourth paragraph*). For a user to receive one or more privileges to perform operations in a database system, the system grants an NPD to a user. (*Page 118, Left column, Second paragraph*). Therefore, *Baldwin* allows a system to combine object privileges together in a group and then assign the group of privileges to a user.

Demurjian also teaches a database system that uses role based security. (*Page 195, Abstract*). *Demurjian* defines three levels of user responsibilities in the system. A "user role" represents a particular privilege assigned to a particular role or job position. (*Page 197, Left column, Third paragraph*). A "user type" represents a privilege that is common to multiple user roles, and a privilege assigned to a user type is passed to each user role. (*Page 197, Left column, Third paragraph*). A "user class" represents a privilege that is common to multiple user types, and a privilege assigned to a user class is passed to each user type and user role in the class. (*Page 197, Left column, Third paragraph*). As an example, *Demurjian* describes a software development environment where different types of employees are allowed to perform different software development functions. (*Figure 2; Page 197, Left column, Fourth paragraph*). The example shown in Figure 2 of *Demurjian* illustrates how different functions may be divided among different types of software engineers and managers. (*Page 197, Left column, Fourth*

paragraph). Overall, *Demurjian* describes a system where privileges may be assigned to an individual job position (a user role), a group of job positions (a user type), and multiple groups of job positions (a user class).

Barkley teaches a workflow management system that incorporates a role-based access control capabilities. (*Abstract*). A “workflow” represents a business process in which documents, information, or tasks are passed between participants. (*Col. 5, lines 46-49*). A user in the system of *Barkley* is assigned a “role,” which represents a job function within an organization. (*Col. 3, lines 60-61; Col. 5, lines 23-27*). The role is also associated with permission to access a resource in the system. (*Col. 3, lines 58-59*). To provide database security during a workflow, the system of *Barkley* activates the roles for the user at appropriate times during the workflow. (*Col. 4, lines 17-22*).

These references allow a system to combine access privileges together in a group and then assign the group of privileges to a user. *Baldwin* and *Demurjian* incorporate the additional feature of grouping privileges together according to job position. *Barkley* incorporates both the grouping of privileges together according to job position and the activation of the privileges at appropriate times during a workflow. All of these references fail to teach or suggest giving one member of a community access to the records of another member based on a management or other type of relationship between the members. The references also fail to teach or suggest giving one member at least a portion of the access privileges of another member based on a management relationship between those members. In addition, these references lack any teaching or suggestion of “automatically” providing access privileges based on relationships between members of the community. Because of this, *Baldwin*, *Demurjian*, and *Barkley* fail to teach or suggest Claims 1, 7, 13, and 16-19.

Baldwin, *Demurjian*, and *Barkley* lack any teaching or suggestion of assigning a single member to multiple positions in a community and then providing managers of those positions with disparate levels of access to the member's records. As a result, these references fail to teach or suggest storing “an assignment of a member ... to a first position” and “an additional

assignment of the member to a second position,” and providing “a manager of the first position with access privileges to records of the member” and “a manager of the second position with disparate access privileges to records of the member” as recited in Claims 1, 16, and 17. As a result, *Baldwin*, *Demurjian*, and *Barkley* fail to teach or suggest Claims 1, 16, and 17.

These references also lack any teaching or suggestion of assigning one management position to another management position and providing a first member with at least a portion of a second member's access privileges based on the assignment. As a result, *Baldwin*, *Demurjian*, and *Barkley* fail to teach or suggest storing “a first assignment of a first member .. to a first manager position,” “a second assignment of a second member ... to a second manager position,” and “a third assignment of the first manager position to the second manager position” as recited in Claims 7, 18, and 19. These references also fail to teach or suggest providing “the first member with at least a portion of the access privileges of the second member” as recited in Claims 7, 18, and 19. In addition, these references fail to teach or suggest giving one member access to the records of another member based on a management relationship between the members. Because of this, these references fail to teach or suggest granting a first member at least a portion of the access privileges of a second member, where the access privileges comprise “access privileges to records of members of the community reporting to the” second member. As a result, *Baldwin*, *Demurjian*, and *Barkley* fail to teach or suggest Claims 7, 18, and 19.

In addition, these references fail to teach or suggest giving one member access to the records of another member and granting disparate access privileges based on the relationships between the members. As a result, *Baldwin*, *Demurjian*, and *Barkley* fail to teach or suggest a processor operable to provide a first member and second member with disparate access privileges to records of a third member based on “recorded assignments” of the “members of the community to positions in the community.” Therefore, *Baldwin*, *Demurjian*, and *Barkley* fail to teach or suggest Claim 13.

For at least these reasons, Applicant respectfully requests withdrawal of the rejections and full allowance of Claims 1, 7, 13, and 16-19, and Claims 2-6, 9-12, 14, and 15 depending

therefrom.

D. THE CLAIMS ARE PATENTABLE OVER RABITTI AND DEINHART

The Examiner rejected Claims 1-15 under 35 U.S.C. § 102(b), as being unpatentable over Rabitti, "A Model of Authorization for Next-Generation Database Systems" ("*Rabitti*"). The Examiner also rejected Claims 1-15 under 35 U.S.C. § 102(e), as being unpatentable over U.S. Patent No. 5,911,143 issued to Deinhart et al. ("*Deinhart*"). Applicant respectfully traverses these rejections for the reasons discussed below.

Rabitti and *Deinhart* each discloses a system that combines database privileges into groups of privileges according to user roles or job positions. *Rabitti* and *Deinhart* also disclose that one role may incorporate or include the authorizations granted to other roles. Access to objects may be granted to a user of the system by assigning the group of privileges to the user.

Rabitti teaches a model of "authorization for next-generation database systems." (*Page 90, First paragraph*). In particular, *Rabitti* focuses on ways of incorporating "implicit authorizations" into a database. (*Page 92, Third paragraph*). Implicit authorizations involve inferring authorization to perform one function based on one or more authorizations to perform other functions. (*Page 92, First paragraph*). As an example, *Rabitti* states that a user who can write information to an object should be able to read the object, so the ability to read the object is an implicit authorization. (*Page 92, Third paragraph*). *Rabitti* allows for the use of role based security in the next-generation database system, where each role corresponds to a set of access authorizations. (*See, e.g., Page 103, Section 3.1*). A parent role includes or incorporates all of the authorizations granted to the children roles of the parent. (*Page 103, Section 3.1*). Therefore, *Rabitti* allows a system to combine object privileges together in a group and then assign the group of privileges to a user, and one group of privileges may incorporate privileges assigned to another group.

Deinhart teaches a role based security system for a database. (*Abstract*). A user in the system of *Deinhart* may hold a job position in an enterprise. (*Col. 7, lines 19-21*). The job

position is “associated with a set of functional tasks,” and each functional task requires access to objects in the system. (*Col. 7, lines 19-21*). The system of *Deinhart* uses the job position of the user to associate the user “with specific access rights to a set of objects” in the system. (*Col. 7, lines 22-26*). To provide database security, *Deinhart* associates a set of access rights with a job position using “role types” and “role instances.” (*Col. 7, lines 26-29*). A role type acts as a template and defines the “types of access rights, objects, and transactions necessary to carry out a set of functional tasks.” (*Col. 3, lines 56-59*). A role instance is derived from a role type, and it defines a set of concrete and specific access rights, objects, and transactions. (*Col. 3, lines 60-62; Col. 7, lines 6-8*). *Deinhart* also teaches the use of parent and child roles, where a parent role may incorporate the access rights granted to the children roles. (*Col. 9, lines 3-12*).

Rabitti teaches an authorization system that uses implicit authorizations and incorporates role based security, and *Deinhart* teaches a role based security system. *Rabitti* and *Deinhart* both fail to teach or suggest giving one member of a community access to the records of another member based on a management or other type of relationship between the members. While *Rabitti* and *Deinhart* use the concepts of parent and children roles in a role based system, these references never teach or suggest automatically providing the parent roles with access privileges to the records of the children roles. Instead, *Rabitti* and *Deinhart* merely teach that the access authorizations of the children roles are also granted to the parent roles. Because of this, *Rabitti* and *Deinhart* fail to teach or suggest Claims 1, 7, 13, and 16-19.

Rabitti and *Deinhart* lack any teaching or suggestion of assigning a single member to multiple positions in a community and then automatically providing managers of those positions with disparate levels of access to the member's records. As a result, *Rabitti* and *Deinhart* fail to teach or suggest storing “an assignment of a member ... to a first position” and “an additional assignment of the member to a second position,” and providing “a manager of the first position with access privileges to records of the member” and “a manager of the second position with disparate access privileges to records of the member” as recited in Claims 1, 16, and 17. Therefore, *Rabitti* and *Deinhart* fail to teach or suggest Claims 1, 16, and 17.

Because *Rabitti* and *Deinhart* fail to teach or suggest giving one member access to the records of another member, *Rabitti* and *Deinhart* fail to teach or suggest providing a first member with at least a portion of the access privileges of a second member, where the access privileges of the second member include “privileges to records of members of the community reporting to the second manager position” as recited in Claims 7, 18, and 19. As a result, *Rabitti* and *Deinhart* fail to teach or suggest Claims 7, 18, and 19.

In addition, *Rabitti* and *Deinhart* fail to teach or suggest giving one member access to the records of another member and granting disparate access privileges based on the relationships between the members. As a result, *Rabitti* and *Deinhart* fail to teach or suggest a processor operable to provide a first member and second member with disparate access privileges to records of a third member based on “recorded assignments” of the “members of the community to positions in the community.” Therefore, *Rabitti* and *Deinhart* fail to teach or suggest Claim 13.

For at least these reasons, Applicant respectfully requests withdrawal of the rejection and full allowance of Claims 1, 7, 13, and 16-19, and Claims 2-6, 9-12, 14, and 15 depending therefrom.

CONCLUSION

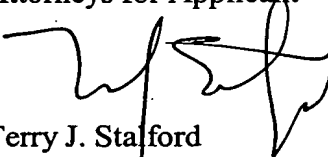
Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests reconsideration and full allowance of all pending claims.

If the Examiner believes a telephone conference would advance prosecution of this case, Terry J. Stalford stands willing to conduct such a telephone interview at the convenience of the Examiner. Mr. Stalford may be reached at 214-953-6477.

Applicant has included an Amendment Fee Transmittal form for the amendments to the claims. Applicant does not believe that any additional fees are due. However, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 05-0765 of Electronic Data Systems Corporation.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant



Terry J. Stalford
Reg. No. 39,522

Please send all correspondence to:

David G. Wille, Esq.
Baker Botts L.L.P.
2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6595

Date: 2/27/01